SECURE COMPUTING

White Paper

www.securecomputing.com

Best practices for monitoring and filtering Internet access in the workplace

Secure Computing has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.

Table of Contents

Secure Computing Corporation
Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters
East Wing, Piper House
Hatch Lane
Windsor SL4 3QP UK
Tel +44.1753.410900
Fax +44.1753.410901

Asia/Pac Headquarters
1604-5 MLC Tower
248 Queen's East Road
Wan Chai Hong Kong
Tel +852.2520.2422
Fax +852.2587.1333

Japan Headquarters
Level 15 JT Bldg.
2-2-1 Toranoman Minato-Ku
Tokyo 105-0001 Japan
Tel +81.3.5114.8224
Fax +81.3.5114.8226

*This document is general in nature and is not intended as legal advice. Counsel should be consulted for specific legal planning and advice. Also, due to the rapidly changing nature of the law in this area, the statues and cases cited should be periodically checked for updates, and thus the material referenced should here not be used as a final or authoritative legal source.

Introduction

This white paper examines the potential legal, security, and human resource problems associated with employee Internet access. Also examined are various approaches to the potential problems associated with employee Internet access including Internet use policies, filtering software, and monitoring software.

Why should employers be concerned about employee Internet use?

Limiting potential liability

The Internet is a powerful tool for business, but if its use is not managed correctly, inappropriate, offensive and illegal content may be just one click away. According to the American Management Association, 27 percent of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems.[1] Research by the Center for Internet Studies shows that more than 60 percent of companies have disciplined employees – and more than 30 percent have terminated employees – for inappropriate use of the Internet.[2]

Organizations that ignore the potential for liability created by workplace Internet abuse can pay a steep price. In August 2003, the Minneapolis Public Library paid $435,000 to settle a sexual harassment claim filed by 12 librarians who said that patrons accessing sexually explicit material had created a hostile work environment.[3] The Chevron Corporation paid $2.2 million to settle a lawsuit by four women who accused the company of tolerating a hostile work environment after receiving Internet pornography from coworkers on company computers.[4]

Another potential source of employer liability is copyright infringement. The liability concerns associated with file-sharing programs in the workplace are not hypothetical. The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) recently sent a letter to all of the FORTUNE 1000 companies warning of "injunctions, damages, costs and possible criminal sanctions," for trading illegal files.[5] The RIAA has already pursued legal action against an Arizona company, winning a $1 million dollar settlement after employees were found to have downloaded thousands of music files on company computers.[6]

Productivity

In addition to expensive liability, inappropriate use of the Internet in the workplace can also cost employers in terms of lost productivity. A study conducted by UCLA found that 60.7% of employees visit Web sites or surf for personal use at work, up from 50.7%.[7] A study conducted by International Data Corp. estimated that 30% to 40% of employee Internet use is not work related. [8]

Why should IT be concerned about employee misuse of the Internet?

Managing internal Internet usage is good security policy

It is well known that the majority of network security problems are internal. According to the SANS institute, 60% of all hacking attacks originate within the organizations.[9] Disgruntled employees have easy access to many hacker Web sites containing hacking tips and tools, which can be used to cause serious damage to company resources.

File-sharing, "malware," etc.

The widespread use of file-sharing peer-to-peer programs has serious implications for IT managers. One study of 15,000 work computers conducted in by eMarketeer found file-sharing software installed on 20 percent of work computers.[10] File-sharing applications are often used to trade copyrighted materials, and can lead to expensive liability for companies, as well as create security problems by opening up employee hard drives to outsiders.

Another problem is "malware," short for malicious software, which are unwanted programs designed to disrupt a computer's operations. Adware, rouge apps, and spyware all fall into this category, and the effects of each can range from annoying to invasive. Free programs available for downloading on the Internet, such as password-helper applications often appear

on employee's computers after they visit certain Web sites, where the software will immediately offer to install itself in what some security experts call a "drive-by download." Some innocuous-sounding "browser toolbar" programs take the "drive-by download" one step further and actually take control of Internet browsers in what security experts call "browser hijacking."[11]

Preserving the cost of bandwidth

With just 15 percent of homes wired for broadband Internet access, many users rely on their employer's high-speed connections to download streaming media files. If employees use their employer's high-speed connections to download Internet movies, streaming media, and MP3 files, the employer's networks could be brought to a halt by the increased traffic and bandwidth demands.

What the law has to say about Internet policies and practices in the workplace[12]

Employers who are considering implementing or who already enforce an e-mail or Internet policy, with or without monitoring and/or filtering software, should have a sense of the legal climate surrounding these policies and practices. We will address a few of these legal concerns in this section. There are, of course, other kinds of legal claims not addressed here that may come up in this type of litigation, including the Federal Electronic Communications Privacy Act, state wiretap laws, the Communications Decency Act, and anti-spam statutes.[13]

Privacy in the workplace

A common legal theory advanced by an employee regarding electronic e-mail and Internet usage arises out of an employee's alleged "privacy interests." A disgruntled employee will often argue that he or she had a reasonable expectation of privacy in his or her workplace e-mail or Internet use, and that the employer intentionally violated this reasonable expectation of privacy by accessing or monitoring the employee's e-mail and/or Web traffic.

A core issue in these cases is whether an employee actually had a reasonable expectation that his or her personal e-mail messages or Web practices were private. Rarely can this be proven. Employers have so far usually won these cases, with some exceptions.

The presence or absence of company e-mail and Internet polices has often influenced the courts in their determination of whether an employee had a legally protectable expectation of privacy. These cases, some of which are described below, underscore the value of an employer having such a policy. In some instances, however, even the lack of a policy may not be fatal to employer access.

In the case of Restuccia v. Burk Technology,[14] the employer had an e-mail policy prohibiting excessive chatting, but lacked any provision about whether employee messages (personal or company-related), were subject to employer oversight. The employees were apparently not told that supervisors had access to their systems, and a company official read a number of employee e-mails over the weekend. Because the employer had no policy, the court found that there was a genuine question as to whether the employees had a reasonable expectation of privacy in their e-mail messages under the Massachusetts privacy act. Accordingly, their privacy claim went forward to trial, but the employer eventually prevailed.

On the other hand, courts are more likely to reject employees' privacy claims where employers have clear, disseminated e-mail and Internet policies. In Bourke v. Nissan Motor Corp.,[15] the court found that employees had no reasonable expectation of privacy where the employees were aware of and, indeed, had signed a waiver acknowledging the company policy restricting use of e-mail to business purposes.

In another employer-friendly ruling in 1996, the Eastern District of Pennsylvania held that even if a company did not have an e-mail policy, employees still would not have had a reasonable expectation of privacy in their work e-mail.[16] Specifically, that Court stated:

"Once [the employee] communicated the alleged unprofessional comments to a second person ... over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, [the company] did not require [the employee], as in the case of urinalysis or personal property search to disclose any personal information about himself. Rather, [the employee] voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interest in such communications."[17]

An employee's consent, whether explicit or implicit[18], may allow an employer to more easily defend against invasion of privacy and other claims.[19] For example, in TBG Ins. Servs. Corp. v. The Superior Court of Los Angeles County, a court held that because the employer had a written "electronic and telephone equipment policy statement" and the employee had consented in writing that his computers could be monitored by the employer, the employee had no reasonable expectation of privacy in a home computer provided by the employer.[20]

Finally, even if a court finds that an employee has a reasonable expectation of privacy in his or her workplace Internet or electronic mail usage, this privacy right will likely be weighed against a company's interest in protecting itself from liability.[21] For instance, if an employee claims to have been sexually harassed by a supervisor through inappropriate e-mail messages, the company has a right and, in fact, an obligation to investigate the sexual harassment claim.

In this situation or other incidents of suspected employee e-mail or Internet misconduct, the company's right to a limited review of the accused individual's particular electronic mail would probably outweigh the possible right to privacy. Other laws may also come into play.

Some state anti-discrimination agencies may even require that sexual harassment investigations include a review of relevant e-mails, and that remedies encompass e-mail policies and oversight, where appropriate.[22]

Free speech in the workplace

In a democratic and open society, employees may feel that their work-related conduct and speech (including e-mail or Internet usage at work) should be entitled to protection under the rubric of "free speech." However, the First Amendment of the United States Constitution generally only prevents government restriction on public debate, not private employer restrictions. For example, the First Amendment has been used to strike down laws that are written so broadly that they prohibit protected as well as unprotected speech.

In Intel Corp. v. Hamidi, an unhappy former employee aired his grievances about the company by repeatedly flooding Intel's e-mail system with spam messages. Intel brought suit under a legal theory of trespass to chattels. The trial court issued an injunction, which prevented the former employee and others acting on his behalf from sending unsolicited e-mail to any addresses on Intel's computer systems.

The former employee appealed the injunction, arguing, in part, that by issuing the injunction the government (through the state court) had violated the First Amendment and prohibited the former employee's free speech. The Appeals Court disagreed.

The Appeals Court stated that the First Amendment protects individuals only from government infringement of speech and, here, what was at issue was a private employer's infringement.[23] The Appeals Court found that judicial enforcement of neutral laws (i.e. laws that do not abridge free speech) through an injunction did not constitute state action and, therefore, did not run afoul of the First Amendment.[24]

This Appeals Court decision was then appealed to the highest state court in California, the California Supreme Court.[25] The California Supreme Court had a very different view of the matter and overturned the injunction, finding that the former employee had not committed a trespass because the computer system was not damaged nor impaired. The California Supreme Court also opined that the injunction would violate the former employee's First Amendment rights.

The high Court found that, although a private employer's refusal to transmit another's electronic speech generally does not implicate the First Amendment, the use of government power, such as through a court injunction, is state action that must comply with the First Amendment. The Court described the injunction as "sweeping" and implied that a prohibition on communication to all Intel addresses was unconstitutionally broad.

The import of this case is difficult to foresee. It continues to be true, however, that private employer curtailment of employee speech generally does not involve the First Amendment. When court involvement is used to assess damages or issue injunctions, the Intel case suggests that the First Amendment may come into play.

Public records access to e-mails

Public employers, such as state and local agencies, boards or schools, should be aware that their business related, and perhaps personal, mail may have to be retained and/or later revealed to others via public records statutes. Generally speaking, public records statutes provide that certain records kept by public employees in the course of their job are accessible by the public upon request and must be maintained.

Each state has promulgated its own public records or public access laws, with various exceptions so that not all documents or messages are available. Accordingly, state and local public or governmental employers should examine their own state's laws to determine their e-mail retention and disclosure obligations.

One controversial issue is whether and to what extent private e-mail generated by public employees on their public employers' computers constitute public records. Recently, the Florida Supreme Court unanimously ruled that the state's open-records law did not encompass public employees' personal e-mail messages.[26]

While this case might herald good tidings for Florida public employers, each state's public records laws vary. For instance, because New York state law eliminates any distinction between the public and private records kept by public officials, the outcome of the case would have been very different in New York, i.e., personal e-mails of New York state employees on state computer systems may be public records.[27]

Drafting an employee Internet use policy

Employers should provide employees with a clear policy statement describing the permitted and prohibited uses of employer e-mail and Internet systems, which include statements that e-mail and Internet messages and traffic on company systems are not the private property of employees. Many employers will also want to state that the employer has the right to - and will - monitor employee e-mail and Internet use.

There are many reasons for such a policy, among which are: 1) to set boundaries for appropriate employee conduct; 2) to clarify employee expectations of privacy; and 3) to foster employee consent, either direct or implied. A clear policy helps reduce legal exposure and bolster employer defenses to employee claims, including for invasion of privacy.

Is Internet content management software right for you?

Filtering software

Filtering software allows employers to select specific categories of Web content to exclude from organization networks. The first generation of Internet filtering software appeared in the mid-1990s. First generation filters were relatively crude instruments that blocked entire Web pages "on the fly" when they contained certain words and phrases such as "sex" or "breast." Consequently, these early filters inadvertently blocked a lot of innocent Web pages.

These early "word blocking" filters were quickly replaced by "list-based" or "URL-blocking" filters that block a regularly updated database of URLs. The databases of these list-based filters are placed into categories, such as "pornography," "gambling," "shopping," "hacking tools," etc. Employers can then select one or more of these categories to block. Most filtering solutions also offer the ability to address file-sharing or "malware" application by blocking the downloading of executable file types.

Studies by the Kaiser Family Foundation and the Department of Justice have documented that list-based filters are highly effective in blocking pornography, with an accuracy of 83 to 98 percent.[28]

Web monitoring software

Monitoring software uses the same technology as filtering software -- a database of URLs grouped into categories, but instead of the URLs being blocked, access is recorded. The log files of URLs accessed are then typically organized by URL, category of URL, workstation, user, and time. This information is then used to create reports of Web access by type or often by individual.

Monitor, filter, both, or neither?

Employers have a variety of choices in implementing software. Some software packages only monitor and produce reports, some only filter, and many provide both functions. Both filtering and monitoring software

have advantages and disadvantages that must be carefully weighed with existing corporate culture before making a decision to deploy one or both.

Use of the Internet can vary widely based on industry and organizational culture, and even by department and job function within the same organization. Take for example, a hypothetical high-tech manufacturing organization with a large, mobile sales force. Shop floor employees in the organization plant have very limited, specific uses for Internet access, suggesting a policy of restricted Internet access. On the other hand, the salespeople who travel frequently with laptops, which are also used for personal reasons while on the road, need freer access.

Some questions an employer should ask before making a decision to purchase filtering and/or monitoring software:

- Do employees use their computers for personal use?
- How wide a variety of sites do employees need to access?
- If the organization is governmental, do state public records laws apply to Internet access logs or e-mail?
- What procedures are there for documenting disciplinary actions?

Filtering software pros and cons

- **Pros:**
  Blocks most (but not all) inappropriate content from employees.
  Generally does not raise privacy concerns.
  Generally does not create discoverable files.
- **Cons:**
  Does not notify employer when abuse has taken place.
  Does not create a record of abuse for justifying disciplinary actions.
  Requires intervention to unblock filtering when sites are overblocked.

Monitoring software pros and cons

- **Pros:**
  Identifies and/or stops some offensive practices.
  Allows employer to identify abusers.
  Creates record to document cause for disciplinary actions.
  Does not block access.
- **Cons:**
  May create discoverable material that could be used in court.
  May create public records for a state or local government agency or entity.
  May lead to privacy issues.
  Can impact employee morale.

What to look for in a filtering and monitoring solution

Compatibility with existing infrastructure

IT managers are usually very busy professionals, challenged with making a disparate collection of hardware and software operate together smoothly. Therefore, a top priority for IT managers adding new components to their networks is ensuring that the new components fit easily with existing hardware and software platforms.

Filtering software typically either is either "natively embedded" on a networked device such as a proxy server, caching appliance, or firewall, or resides by itself on a dedicated server running a variant of the Windows, Unix, or Linux operating systems. The most popular filtering vendors offer a variety of options for use with different networking platforms that work with the more widely used networked devices. Which choice is best depends on the individual network.

An extensive, high quality database

The heart of a filtering solution is an extensive database of URLs sorted into categories. The most widely used filtering solutions contain millions of URLs sorted into dozens of categories.

Additionally, most filtering solutions can address unwanted applications and files, such as file-sharing, "malware", and peer-to-peer by blocking the downloading of executable files and other file types, such as .MP3s.

Flexible filtering options

In order to meet the needs of an organization, a filtering solution needs to have the flexibility to handle multiple levels of filtering for different personnel and departments.

The most widely used filtering solutions offer the ability to select individual users, groups of users, individual workstations, or groups of workstations for a specific level of filtering using a defined set of filtering categories. These filtering solutions also allow employers to combine filtering and monitoring within the same user or group of users.

Ability to monitor, filter, report

The more widely used filtering solutions offer a variety of options for both monitoring and filtering. These solutions allow an administrator to select for example, filtering of pornography for all users at all times, filtering of other non-work sites during the work day for some users and, monitoring for other groups of users. The best filtering solutions build in all these options, so that employers can adjust levels of filtering and monitoring as need arises.

For more information

To find out more about Secure Computing's versatile filtering products and the advantages of managing your organization's Internet access and activity, contact Secure Computing today at 1 800 692-5625 or visit them on the Web at *www.securecomputing.com.*

Endnotes

1 American Management Association, "2001 Workplace Monitoring and Surveillance: Policies and Practices," 2001.

2 Center for Internet Studies, "Internet use in the workplace," January 2000.

3 Associated Press, "Minn. Librarians Settle Internet Case," August 15, 2003.

4 Associated Press, "Chevron Settles Harassment Lawsuit for $2.2 Million," February 21, 1995.

5 Associated Press, "Hollywood targets corporations to fight illegal downloading," February 13, 2003.

6 Newsbytes News, "Tech Firm Nailed For Internal MP3 Sharing," April 10, 2002.

7 UCLA Center for Communication Policy, "The UCLA Internet Report," 2001.

8 IDC, "Worldwide Market for Internet Access Control," 2000.

9 SANS Institute, 2001

10 eMarketeer, 2000.

11 Wired News, "Sneaky Toolbar Hijacks Browsers," January 30, 2003.

12 Reprinted with permission by Mark E. Schreiber, Esq. of Palmer & Dodge LLP

13 Mark E. Schreiber, *Employer E-Mail and Internet Risks, Policy Guidelines and Investigations*, 85 MASS. L. REV. 74 (Fall 2000); *see also Pharmatrak, Inc. v. Pharmatrak, Inc.*, No. 02-2138, 2003 WL 21038761 (1st Cir. May 9, 2003).

14 No. 95-2125, 1996 Mass. Super. LEXIS 367 (Mass. Super. Ct., Aug. 12, 1996).

15 No. BO68705, (Cal. Ct. App. July 26, 1993), unpublished, but available at *www.loundy.com/CASES/Bourke_v_Nissan.html.*

16 *Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

17 *Smyth*, 914 F. Supp. at 101.

18 *See Watkins v. Barry*, 704 F. 2d 577 (11th Cir., 1983).

19 *See Stewart v. The Pantry Inc.*, 715 F. Supp. 1361, 1368 (W.D. Ky. 1988) ("consent...is a complete defense"); *Wal-Mart, Inc. v. Stewart*, 990 P.2d 626, 632 (Alaska 1999) (discussing the employer's consent defense, trial court instructed the jury "that any search to which [the employee] had voluntarily consented could not be considered an offensive intrusion"). *But see Kraslawsky v. Upper Deck Co.*, 56 Cal. App. 4th 179, 193 (Cal. Ct. App. 1997) ("consent is generally viewed as a factor in the balancing analysis, and not as a complete defense to a privacy claim").

20 96 Cal. App. 4th 443, 445 and 452-54 (Cal. Ct. App. 2002).

21 *See e.g. Garrity v. John Hancock Mutual Life Ins. Co.*, No. CIV.A.00-12143-RWZ, 2002 WL 974676, at * 2 (D. Mass. May 7, 2002).

22 *See* Massachusetts Commission Against Discrimination, Sexual Harassment in the Workplace Guidelines (Oct. 2, 2002), available at <www.state.ma.us/mcad/shguide.html#VI>.

23 *Intel Corp. v. Hamidi*, 94 Cal. App. 4th 325, 337-41 (Cal. Ct. App. 2001).

24 *Intel Corp*, 94 Cal. App. 4th at 337-41.

25 *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (Cal. 2003).

26 *Times Publishing Co. v. City of Clearwater*, No. SC02-1753 (Fl. Sept. 11, 2003).

27 Andrew Harris, *Private E-mail is Out of Reach*, THE NATIONAL LAW JOURNAL, Sept. 22, 2003, at 5.

28 Kaiser Family Foundation, "See No Evil: How Internet Filters Affect the Search for Online Health Information," December 10, 2002. & " U.S. Department of Justice: Web Content Filtering Software Comparison," eTesting Labs, October, 2001.